ARITHMETIC CIRCUIT TO INCREASE THE SPEED FOR A MODULAR MULTIPLICATION FOR A PUBLIC KEY SYSTEM FOR ENCRYPTION

Abstract

A circuit and a method for solving the Montgomery multiplier bottleneck problem encountered during a memory access using two ports or single port general-purpose memories is described. A first and a second memory are provided such that variables that are stored in one memory must be read for an operation to be recorded in the second memory. Thereafter, during a reading cycle corresponding to a pipeline process, certain of the variables are read from the first memory and are loaded in the predetermined register while the other variables are read from the second memory and are loaded in the remaining registers.